CEP Magazine - March 2021
Brazil's general data protection law: What has it done?

By Marcelo Crespo, PhD, CCEP-I, and Guilherme Beloto

Marcelo Crespo (marcelocrespo@pgadvogados.com.br) is a partner specializing in digital law at PG Advogados in São Paulo, Brazil. **Guilherme Beloto** (gcbeloto@gmail.com) is a political scientist and lawyer based in Luxembourg, currently specializing in privacy and data protection.

In January 2020, we published an article on the key challenges in developing a privacy compliance program in 2020 (and beyond).[1] At that time, we urged organizations to overcome the difficulties of implementing such a program, as there was a pressing need to comply with data protection laws that were becoming increasingly available, and, specifically in Brazil, it was expected that such a law would come into force.

Now let us look at what has happened over the past year regarding Brazil's move toward data protection legislation and what we can expect for the future.

A brief history of the LGPD

Lei Geral de Proteção de Dados[2] (LGPD) is the Brazilian equivalent of the European Union's General Data Protection Regulation[3] (GDPR). It is the national data protection regulation in Brazil, valid throughout the country. Its origins can be traced back to 2010, when the federal government created an online platform to receive opinions via a public consultation, gathering suggestions on what a data protection legislation should entail. A second round of consultations occurred in 2015.

By 2016, the federal government considered itself ready and sent a bill to be discussed in Congress, and, in 2018, it enacted the LGPD. Initially, the legislation foresaw a transition period for organizations to adapt and acquire compliance to the new requirements. The LGPD was planned to enter into force in February 2020; before that deadline was reached, however, the president enacted a provisional measure (*Medida Provisória*) that delayed the implementation of LGPD by six months.[4]

And then...COVID-19 changed the world. And with the global pandemic, the legislator decided to postpone the entry into force of the LGPD once more. After amendments to the original text, the final version of the LGPD finally came into force on September 18, 2020. Administrative fines will apply as of August 2021.

An overview of the LGPD

It is essential to realize that data protection legislations are not only about personal data breaches or security incidents, though these are essential topics to consider when analyzing them. It should be expected that, at some point, every organization will face a personal data breach. We have been advocating for some time now that organizations should engage this topic with a hands-on approach, as the denial only delays essential preparatory work that should enable the organization to quickly tackle the challenges that come with a data breach.

The Brazilian legislation also addresses information security, which is closely connected to (personal) data protection and highlights the need to protect fundamental rights, specifically freedom, privacy, and the free development of the personality of individuals (Article 1, LGPD):

The legislation is structured in 10 chapters:

- Chapter I: Preliminary provisions
- Chapter II: Processing of personal data
- Chapter III: Data subjects' rights
- Chapter IV: The processing of personal data by the public authorities
- Chapter V: International data transfer
- Chapter VI: Personal data processing agents
- Chapter VII: Security and good practices
- Chapter VIII: Supervision
- Chapter IX: The National Data Protection Authority (ANPD) and the National Personal Data Protection and Privacy Board
- Chapter X: Final and transitional provisions

In a similar way to the GDPR, the LGPD does not prevent the processing of personal data in an absolute way. On the contrary, it merely requires that organizations have proper governance over the personal data being processed. Privacy is being protected by the protection of personal data.

It is important to differentiate privacy both as a "negative" and as a "positive" right. Briefly put, in the former, there is an essential individual dimension to be free from abuse, embarrassment, and physical harm. It is every person's right to be able to withdraw from public life, the right to be left alone. In its positive conception, it is the right to act, and in the context of this article, it is the right to have the data that can identify oneself. This concept is intertwined with the personal life of the individual and adds a layer of procedural aspects.

The LGPD is based on a series of principles laid down in Article 6. Most of them have a parallel with the principles of the GDPR, such as lawfulness, purpose limitation, data minimization, accuracy, integrity and confidentiality, and accountability. The two main differences are that (i) free access, which is a *principle* in the LGPD laid down in Article 6(IV) is considered a *right* in the GDPR (Article 13), and (ii) storage limitation, a *principle* in the GDPR set forth in Article 5(1)(e), is in Article 16 of the LGPD as the *obligation* to delete personal data after processing is finished. Although it might be easier to enforce a provision that commands an obligation, a *principle* must always be observed. This difference, which seems small, may imply a different kind of response to the national authority.

Being mainly based on principles, the LGPD lacks some of the specific instructions that can be found in other data protection legislation. Article 2 provides for the basis of the data protection, such as the respect for privacy; informative self-determination; freedom of expression, information, communication, and opinion; inviolability of intimacy, honor, and image; economic and technological development and innovation; free enterprise, free competition, and consumer protection; and human rights, the free development of personality, dignity, and the exercise of citizenship by natural persons.

Lawfulness of processing: LGPD vs. GDPR

After two years of the GDPR, most people have heard about the lawfulness of processing; that is, for the

processing of personal data, which includes any operation or set of operations performed on personal data or on sets of personal data, organizations need to have at least one of the legal bases provided for in Article 6 of GDPR, such as consent of the data subject, compliance with a legal obligation, etc. Article 9 of the GDPR addresses the processing of special categories of personal data, such as the ones revealing racial or ethnic origins, political opinions, etc. The LGPD uses the same approach and provides for 10 legal bases for processing of personal data in Article 7, whereas Article 11 provides for the legal bases for the special categories of data.

However, content-wise, the LGPD and GDPR differ significantly in this respect. A brief comparison to the GDPR reveals, for example, that the LGPD does not allow processing when necessary in order to protect the vital interests of the data subject or of another natural person (Article 6(1)(d) of the GDPR), or when necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6(1)(e) of the GDPR). In turn, LGPD allows the processing for studies by a research body (Article 7(IV)) for regular exercise of rights in judicial, administrative, or arbitral proceedings (Article 7(VI)); for the protection of health in procedures carried out by health professionals, health services, or health authorities (Article 7(VIII)); and for credit protection (Article 7(X)), which addresses the need of score credit bureaus and financing.

It is also worth noting that in regard to the special categories of data, the LGPD does not allow the processing laid down in Article 9(2)(d) of the GDPR when carried out in the course of legitimate activities with appropriate safeguards by a foundation, association, or any other nonprofit body, or the processing of personal data that were manifestly made public by the data subject, as is the case in the GDPR in Article 9(2)(e). In turn, LGPD allows the processing of sensitive personal data to ensure the prevention of fraud and security of the data subject (Article 11(II)(g)).

The lack of possibility in the LGPD for processing personal data that is carried out in the public interest or when personal data were manifestly made public by the data subject (for special categories of data) creates a conundrum. Although it may seem a mere theoretical issue at first sight, some controllers may face difficulties supporting their processing.

A case demonstrating this challenge for controllers falling under the scope of the LGPD is the use of democratic oversight of political opinions. In the past few years, some start-ups have used artificial intelligence analysis of political speeches and opinions to create insightful breakdowns of politicians' positioning in the political spectrum, or inconsistencies of political opinion and political votes in Congress. The data being used (political speeches and opinions) are personal data by nature (i.e., information relating to an identified or identifiable natural person, as defined in Article 4(1) of the GDPR and Article 5(I) of the LGPD). Although such personal data were manifestly made publicly available by the politicians during their speeches, one could argue that the LGPD lacks a provision allowing this processing.

Privacy compliance program

Another aspect that reveals the lack of specific recommendations in the LGPD can be found when controllers try to address the need for creating and maintaining a privacy compliance program. Article 50 provides for the possibility of controllers or processors—individually or in associations—to create guidance of best practices and governance, as well as technical standards, specific obligations, procedures for data subject requests, and complaints and internal mechanisms for oversight of their operations, among others. Nevertheless, if controllers or processors decide to create a privacy compliance program, the minimum requirements would be the following:

- Demonstration of the commitment to adopt internal processes and policies that ensure compliance to the legislation and best practices.

- Application of the program to the entire set of personal data under their control, considering the structure, scale, and volume of processing and data sensitivity.
- Establishment of policies and safeguards based on systematic risk assessments.
- Establishment of a trusted relationship with the data subject.
- Integration with the general governance structure, with internal and external supervisory mechanisms.
- Creation of an incident response and remediation plan.
- Constant updates to the program.

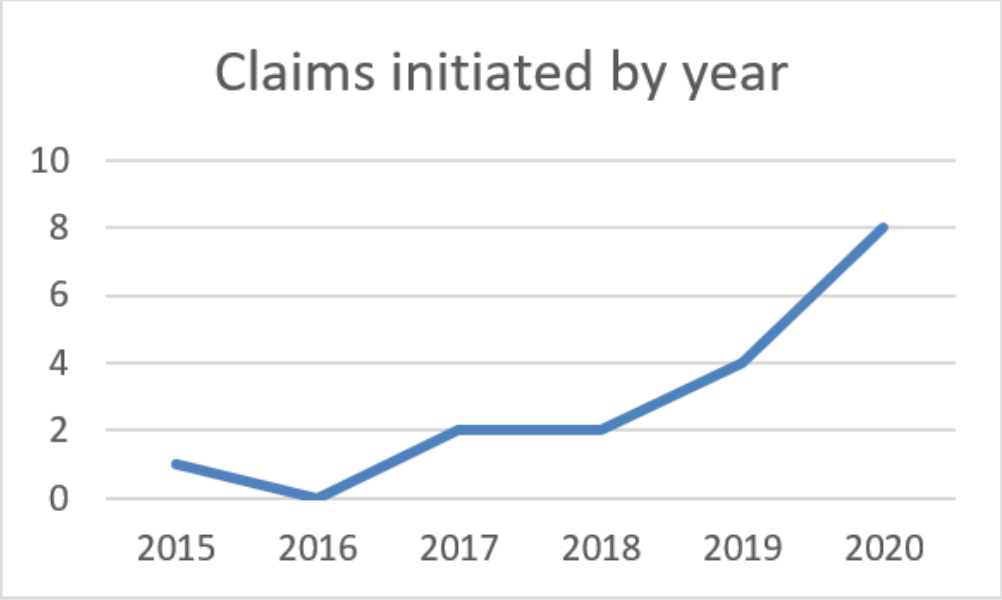
Thus, considering that a privacy compliance program is not mandatory, its existence should be considered by the national authority in case of sanctions, as provided for in Article 52, §1º, IX, LGPD.

LGPD applied in practice

The LGPD has been in force in Brazil since September 18, 2020, but consumer protection bodies and public prosecutor's offices across the country were using the LGPD to support their claims before it was law. Thus, we found ourselves in a twofold situation: the official supervisory body, the Autoridade Nacional de Proteção de Dados (ANPD)—the Brazilian National Data Protection Authority—was not fully operative, and the LGPD was being used to support claims of compliance to a legislation that was still in *vacation legisie* (the period between the enactment and coming into force).

In this context, the favorite method used was to take legal action, with public actions brought by the public prosecutor's office. According to the "Violations Portal" maintained by the National Association of Data Privacy Professionals (ANPPD), there were 17 claims regarding data protection spread over the past five years (Figure 1).[5]

Figure 1: Data protection claims, 2015–2020.



Year	# claims
2015	1
2016	0
2017	2
2018	2
2019	4
2020	8

It is easy to notice the growth of legal actions since the entry into force of the LGPD, as six new claims were initiated in only two months. Furthermore, several claims mentioned the LGPD to support their arguments, even

those that were brought before the legislation was in force.

One of these legal claims was brought by the Public Prosecutor's Office from Brasilia, capital of the country. The Ministério Público do Distrito Federal e Territórios (MPDFT) tried to stop Serasa S.A., a company that provides support services in relation to credit decisions, from selling personal data. The organization was originally created by the Brazilian Federation of Banks (Febraban), but it is currently owned by the Irish group Experian. It argued that by selling personal data for customer prospecting, including contact details and information about sex, age, purchasing power, social class, location, affinity models, and risk screening, Serasa was in violation of the Federal Constitution, Civil Code, Consumer Protection Code, Civil Rights Framework for the Internet, and the LGPD. After the first judicial decision that was in favor of the company, Serasa had to refrain from selling personal data after the appellate decision. The judge's argument is remarkable, as it ignores the nine possibilities of lawful processing other than consent: "This is because according to Article 7, I, of Federal Law 13.709/18, known as Lei Geral de Proteção de Dados - LGPD, processing of personal data may only be carried out with the consent of the data subject."[6]

As one can foresee, there is a long way to go for data protection in Brazil, insofar as judges themselves are still confused by the possibilities of the new legislation.

LGPD: The economic advantage

As follows from this brief analysis of the LGPD, the Brazilian legislation does not provide for specific instructions on how to comply, and controllers and processors can only tap broad directions. The beauty of this legislation, however, is that the easiest way to comply with it is to create a robust privacy compliance program that adapts to the innovations and modifications that time will bring, especially after the national authority starts issuing guidelines and clarifying additional points of the legislation, which will bring new understanding and guides in the future.

The LGPD does not intend to hinder businesses or bureaucratize the operations of organizations. It is therefore necessary to take a proeconomic reading of the law. Controllers and processors that develop a privacy compliance program will ultimately be at the forefront of protecting the privacy of data subjects and their own business. It is therefore essential that the national authority brings light to the doubts regarding the application of the LGPD, while controllers and processors should avail themselves of best practices, whether national or international, to ensure the continuity and prosperity of their business in this new era. After all, doing business in a privacy-compliant fashion is likely to become—and should be considered—a competitive advantage.

About the authors

Marcelo Crespo has a doctorate in criminal law from the University of Salamanca (Spain). Marcelo coordinates the post-graduation area of digital law and compliance at Damásio Educacional, and he is an international speaker and author of several publications in digital law, data protection, and compliance.

Guilherme Beloto assists national and international companies based in Brazil with national and international data protection law compliance.

Takeaways

- The *Lei Geral de Proteção de Dados* was inspired by the General Data Protection Regulation, but its specificities cannot be overlooked.
- Privacy compliance can be used to improve business and brand recognition among consumers and

business partners.

- Do not postpone starting your compliance measures, because it usually takes longer than anticipated.
- Privacy compliance is not as simple as checking legislation requirements. You must implement a comprehensive privacy compliance program that will tackle current and future data protection necessities.
- Do your homework, and when the inevitable happens (i.e., when a data breach occurs), you will have the tools to properly address it.

1 Marcelo Crespo and Guilherme Beloto, "Privacy compliance challenges in 2020 and beyond," *CEP Magazine*, January 2020, http://bit.ly/3b7mhIt.
2 Lei Geral de Proteção de Dados Pessoais, nº 13.709/2018 (Braz. 2018), https://lgpd-brazil.info/.
3 Council Regulation 2016/679, General Data Protection Regulation, 2016 O.J. L119, https://gdpr-info.eu/.
4 Medida Provisória n° 959/2020 (Braz. 2020).
5 "Portal das Violações – LGPD," Associação Nacional dos Profissionais de Privacidade de Dados, accessed January 14, 2021, https://anppd.org/violacoes.
6 Ministério Público do Distrito Federal e Territórios v. Serasa, no. 0749765-29.2020.8.07.0000, November 23, 2020, https://bit.ly/2N5w2gm.